CLAIMS

1. A biometric authentication system comprising:

a mobile storage device with a computing function having a tamper-resistance; and

a reader/writer having a tamper-resistance for reading/writing information from/into said mobile storage device,

wherein said reader/writer includes:

a biological information input device for inputting biological information,

preprocessing the biological information inputted by said biological information input device, and

transmitting intermediate information thus preprocessed to said mobile storage device, and

wherein said mobile storage device includes a template of biological information and a secret key to be used for electronic authentication;

compares said intermediate information with said template; and

makes said secret key available upon a match after comparing.

2. A biometric authentication system according to Claim 1, wherein,

said biological information is fingerprint information,

said reader/writer transmits, sequentially to said mobile storage device, a fingerprint image information necessary for a fingerprint identification, and

said mobile storage device performs the fingerprint identification by processing said fingerprint image information sequentially.

3. A biometric authentication system according to Claim 1, wherein,

said biological information is fingerprint information,

information for correcting a positional displacement between a registered fingerprint recorded in said template and an input fingerprint that is newly inputted is calculated by using a core position of the fingerprint,

a small image in the vicinity of a featuring point of said registered fingerprint is retrieved by performing matching in the vicinity of coordinates of an image of said inputted fingerprint, the positional displacement of the coordinates having been corrected, and

said fingerprint image is determined to be identical to said template according to the number of matched small images.

4. A biometric authentication system according to Claim 3, wherein,

a normal vector of a ridge is retrieved, and

a position where said normal vector largely changes is determined as a core of the fingerprint.

5. A biometric authentication system according to Claim 1, wherein,

said biological information is fingerprint information,

information for correcting a positional displacement between a registered fingerprint recorded in said template and an input fingerprint that is newly inputted is calculated by forming images having specific luminance distributions in the peripheries of individual featuring points with regard to the input fingerprint and the registered fingerprint, and by correlating said images therebetween,

a small image in the vicinity of a featuring point of said registered fingerprint is retrieved by performing matching in the vicinity of coordinates of an image of said inputted fingerprint, the positional displacement of the coordinates having been corrected, and

said fingerprint image is determined to be identical to said template according to the number of matched small images.